Seeing through the Eye of God

Valentina Golunova 2021-03-30T11:25:41

Telegram is a powerful tool for end-to-end encrypted communication and one of the most popular messenger apps in Russia. However, one aspect often evades public attention: Telegram is swamped with bots which gather and disseminate personal data. Roskomnadzor, Russia's media watchdog, has just moved to block one of the prominent bots, proudly named 'Eye of God'. It allows users to acquire personal data of Russian nationals available through both publicly accessible and leaked databases. In response to Roskomnadzor's move, the bot's developers made changes to its operation which, nevertheless, hardly make Eye of God compliant with data protection legislation.

While Telegram bots offer certain positive implications through the newfound transparency they afford, these do not override the tremendous privacy risks posed. But even more importantly, there is little the Russian authorities can do to force Eye of God and other bots to respect the rights of data subjects.

Background

Telegram bots are small apps embedded in chats or channels which can be used to automate queries. First introduced in 2015, bots have quickly gained popularity, as they allow users to create customised tools and build integration services. It did not come as a surprise that Telegram bots are not only used by good-faith developers, but were also co-opted by scammers and criminals. This is how Telegram bots have become an integral part of the grey market for Russian nationals' personal data of Russian nationals. Some of these bots can find out a person's name by their phone number. Others have even more sophisticated functions. Eye of God enables its users to look for information about any Russian national by a wide array of parameters. Some data sourced by the bot, such as a person's name or image, is publicly accessible, for example, on social media platforms like VKontakte or Facebook. However, Eye of God also offers an opportunity to search for confidential data, including information about traffic fines and bank loans, illegally leaked by low-level employees at police departments and credit organisations.

Eye of God v. Roskomnadzor

For a long time, Russia's law enforcement agencies abstained from taking any firm action against Telegram bots trading in personal data. However, it all changed on 9 March 2021, when Roskomnadzor issued a request to Telegram's administration to block all bots violating Russian data protection legislation. Upon Telegram's failure to comply, on 12 March 2021, Roskomnadzor proceeded to block some of the most popular bots, including Eye of God, in Russia. The bot's developers objected to the action taken and sought legal assistance from the Net Freedoms Project, a civil

rights NGO, whose lawyers promptly filed a request to Roskomnadzor demanding legal justification of the blocking.

While Roskomnadzor is still to provide its response, the bot's developers have issued a press release. On the one hand, they denied having breached data protection law, as the bot operates as a search engine which merely processes publicly accessible data. On the other hand, the press release points to a number of actions taken by the bot's developers to meet Roskomnadzor's demands. According to the bot's spokesperson, Eye of God has undergone an audit of its internal documentation and is now run as an LLC listed in the registry of data controllers collated by Roskomnadzor. Access to the bot is now allegedly restricted to specific categories of users, including journalists, witnesses of events which have a direct impact on the vital interests of data subjects and other individuals (including traffic accidents or crimes), employees of credit organisations and law enforcement agents. Eye of God also introduced an authentication procedure to ascertain whether its users have a lawful ground for accessing data. Finally, individuals located outside of Russian territory and not accredited as journalists may no longer use the bot.

Analysis

Roskomnadzor's move to block Eye of God and the like are presumably inspired by the amendments to the Federal law 'On Personal Data' (N 152-FZ) which came into force on 1 March 2021. According to the newly introduced Article 10.1, any party involved in the dissemination of personal data made publicly available as a result of a crime, administrative offence or *force majeure* must account for the lawfulness of such dissemination. Therefore, Eye of God is no longer allowed to escape responsibility for drawing information from leaked databases. Interestingly, Article 10.1(2) 'On Personal Data' clarifies that the same duty arises when the personal data was made publicly available by the data subject themselves. Consequently, Eye of God is also restricted from scraping data available on social media platforms without explicit consent of the data subject. Eye of God's business model directly contravenes these provisions.

Nevertheless, according to the bot's spokesperson, Eye of God considers itself nothing more than a search engine which merely facilitates the collection of information that could otherwise be gathered manually. Contrary to the EU's approach, Russian law does not recognise search engines as data controllers, which could provide Eye of God a certain leeway. However, Eye of God does not seem to fall within the definition of the search engine given under Article 2(20) of the Federal law 'On Information, Information Technologies and Information Protection' (N 149-FZ), which defines search engines as systems whose function is limited to providing links to websites which store specific information. The bot does more than that: it offers a short report about the person indicated in the search query. In effect, Eye of God should be regarded as a data controller and most certainly remains in breach of Article 22(1) of the Federal law 'On Personal Data', which requires all data controllers to be listed in the special register kept by Roskomnadzor. Contrary to Eye of God's claims, Eye of God's website reveals that the bot is still run by the sole proprietor, which is not officially recognized as a data controller, and not an

LLC featured in the register. This gives rise to a suspicion that Eye of God simply provided false information in its press release.

Eye of God's developers also insist on the lawfulness of its operation, as data subjects give explicit consent to the processing of all the data sourced by the bot, for instance, while concluding a service agreement with a bank or an insurance agency. However, this statement runs contrary to the fundamental principle of purpose limitation codified under Article 5(2) of the Federal law 'On Personal Data'. Even if the data subject gives consent to processing of their personal data for a specific purpose, this data cannot be processed in a manner that is incompatible with this purpose. Further, Article 12(3) of the Federal Law 'On Personal Data' obliges the data controller initiating a cross-border transfer of personal data to make sure that the foreign state offers an adequate level of data protection. While Eye of God claims to only provide access to users within the Russian territory, in reality it authenticates everyone whose account is linked to a Russian phone number, regardless of whether this person is located in Russia or abroad. In addition, experts emphasise that Eye of God violates the data protection legislation as it does not allow data subjects to request erasure of their personal data in accordance with Article 14(1) of the Federal law 'On Personal Data'.

Regardless of the glaring insufficiency of measures taken by Eye of God's developers, the Russian authorities would presumably be unable to take further action against the bot. Less than hour after Roskomnadzor blocked Eye of God, the bot became available via a backup solution. Since the developers can circumvent the restrictions so easily, the fear of legal responsibility will likely not stifle their activities. Therefore, Eye of God would probably continue disseminating personal data in breach of Russian data protection law, despite the ostensible willingness to meet Roskomnadzor's demands.

Broader perspective

Apart from specific data protection issues and regulatory hurdles, the onset of Telegram bots gives rise to the dilemma of how to strike a fair balance between protecting personal data and ensuring a reasonable degree of its availability for the benefit of public interest. Indeed, Telegram bots have provided incredible opportunities for investigative journalism in Russia. However, unrestricted access to personal data via Telegram bots has also led to many abuses, such as the blackmailing of Russian nationals and the planning of large-scale scammer attacks. Even if it were confirmed that Eye of God is just a data aggregator and does not bear the duties of a data controller, the privacy concerns would certainly persist. The public outcry provoked by Clearview AI, which helps match faces to a large database of images scraped from the Internet, exposes the resistance towards the unrestricted use of publicly available data for identification purposes. Therefore, the intrusive features of Telegram bots are unlikely to outweigh their potential upsides.

The recent events also reveal the Russian government's hypocritical approach towards the protection of privacy. For years, Roskomnadzor has been waging war on encryption, thus potentially encroaching on the confidentiality of correspondence

guaranteed by Article 8 of the European Convention on Human Rights. Today, in contrast, it pursues a privacy agenda to crack down on Telegram bots which violate the rights of data subjects. Unless the Russian authorities align their policies and put forward a coherent strategy for protection of personal data on the internet, these contradictions are going to remain unaddressed.

But even then, there is little hope that Russia would manage to tackle the flagrant privacy concerns outlined. One may argue that data protection legislation is simply not fit for purpose to rein in elusive Telegram bots. But, in fact, the problem stems from the limited impact of blocking measures, which authorities could impose, as well as the inability to track down the bot's developers, who could reside anywhere on Earth. While the government can move to block one specific bot, it cannot eradicate thousands of its copies that would be put back online in a split second. The same obstacles often arise in intermediary liability disputes. While courts strive to make platforms take a more proactive stance against illegal content online, the truth is that such content spreads at such a pace that no injunction can restrain it. This controversy reflects an increasing divide between substantive legislation and its effective enforcement in the digital dimension.
